Data Theft, Loss, and Misuse Panel Testimony

Michael Mellor
Deputy Chief Information Security Officer
Centers for Medicare and Medicaid Services

Questions:

1. ***Briefly describe your organization and your information security approach to data theft, loss, and misuse.***

The Centers for Medicare & Medicaid Services (CMS) is the agency of the Federal Government, which administers the Medicare and Medicaid programs. In this capacity, CMS is responsible for the payment of over $700 billion each year for medical services rendered to the nearly 92 million program beneficiaries and recipients. CMS has become the largest purchaser of health care in the United States, serving over 92 million beneficiaries, almost one in three Americans. CMS currently has approximately 4,900 employees at its central site in Baltimore, and in 10 Regional Offices in major cities throughout the country. CMS contracts with approximately 30 companies to process claims for reimbursement for medical services rendered under the Medicare program, and works with all states and territories in the management of the Medicaid program.

In the administration of these programs, CMS utilizes many assets, including buildings, facilities, communications equipment, computer systems, employees, contractors, public trust, and information. A loss of any one of these assets could affect the quality of support provided by CMS to its various customers. CMS collects information that falls into the categories of privacy data, proprietary data, procurement data, inter-agency data, and privileged system information. Access to these types of information is controlled by the Privacy Act of 1974, as amended, The Medicare Prescription Drug, Improvement and Modernization Act (Section 912) of 2003, and the Federal Information Systems Management Act of 2002 (FISMA), as well as various rules, regulations, policies and guidelines promulgated by the Department of Health and Human Services (DHHS), the Office of Management and Budget (OMB), and the National Institute of Standards and Technology (NIST). As a result, CMS has a legal and practical responsibility to maintain the confidentiality, integrity, and availability (CIA) of this information.

The CMS approach to protecting against data theft, loss, and misuse involves various people, technology, and operations countermeasures. CMS policy requires the establishment of automated mechanisms which provide the ability to generate an audit record for a pre-defined set of events that are adequate to support after-the-fact investigations of security incidents to include data theft, loss, and misuse. These events include access to and modification of files. Information system audit records are reviewed and analyzed to identify and detect unauthorized, inappropriate, unusual, or suspicious activity no less than once every 24 hour period. Administrator groups are inspected on demand but at least once every seven days to ensure unauthorized administrator accounts have not been created. Manual reviews of system audit records are performed randomly on demand but at least once every 30 days. Any unauthorized, inappropriate, unusual, or suspicious activity is investigated and

reported to appropriate officials, in accordance with current CMS Incident Handling and Breach Notification/Analysis Procedures.

The CMS approach to data theft, loss and misuse is focused on prevention and detection through a defense-in-depth and risk based approach (as required by FISMA) to IT systems security.

a. People
    i. Policies and procedures
    ii. Training and awareness
    iii. System security administration
    iv. Physical security
    v. Personnel security
    vi. Facilities countermeasures
b. Technology
    i. IA architecture
    ii. IA criteria (security interoperability)
    iii. Acquisition/integration of products
    iv. Risk assessment
c. Operations
    i. Security policy
    ii. Certification and accreditation
    iii. Security management
    iv. Key management
    v. Readiness assessment

2. Provide one or two examples of information security issues you have faced recently related to data theft, loss, and misuse, and describe how you addressed these issues.

Without going into specifics, the CMS information security policies require that all CMS information systems are continuously monitored to provide real time detection, identification, and alerting of potential security incidents and compromises. CMS also maintains and promotes contact with outside information security groups in order to further organizational knowledge of potential threats.

The CMS information security policies require that all CMS information systems develop, implement, and maintain incident response policies and procedures. Automated incident handling mechanisms to include identification, containment, eradication, recovery, and follow-up capabilities are in place. All CMS information system users must receive both general and specialized training on incident response annually. All incident response procedures are tested and updated annually.

3. What kinds of trade-off's have you had to make between security and usability, and other operational considerations?

As a government agency, our focus is to provide benefits information and services to citizens, in particular, healthcare services and beneficiary services information to the over-65 population and other vulnerable populations of the United Sates. As such, the demographics of our beneficiary population do not necessarily allow the use of more complex and sophisticated identity management tools and processes (such as hard-tokens, complex multi-factor e-authentication mechanisms, or other technologies that may add undue complexity on the user experience.)

However, we must ensure that, depending upon the scope and sensitivity of data being accessed, that sufficient controls are in place to ensure the confidentiality of data, particularly personally identifiable data, without placing an undue burden on the user population.

As a federal agency, CMS is subject to the security control requirements specified through FIPS 199 and FIPS 200 (and all of the associated NIST 800-series special publications as mandated by FISMA.) During the course of application development and deployment, business processes must sometimes be modified to limit the amount of data being presented (through certain access portals) in order to maintain the confidentiality of the data, while still providing sufficient usability to achieve mission objectives. These trade-offs can sometime be challenging. The scope of trade-offs vary from modification of business processes to limit data being accessed, to increasing the risk tolerance threshold for certain applications and systems.

4. ***What information security standards are you currently using to protect your business from data theft, loss, and misuse?***

For CMS, privacy and security for sensitive data is addressed in several legislative requirements as well as industry and cross-industry standards. Of particular concern is the transfer of Health Insurance Portability and Privacy Act (HIPAA) covered Electronic Personal Health Information (ePHI). The security and privacy requirements for the protection of ePHI are promulgated through several legislative mandates and their accompanying standards, the most encompassing being HIPAA. However, when the data is received, generated, or aggregated on the CMS/Federal side, additional requirements are immediately applicable and are enforced. These additional requirement sets, such as those mandated under the Federal Information Security Management Act (FISMA) may require special configurations when interfacing with non-government (such as HIO or NHIN) systems. Many of the government mandated standards (typically defined under NIST guidance) are more stringent than their commercial equivalents (such as the requirement to use encryption modules that are certified by NIST laboratories for data encryption). Below is a sampling of federal and non-federal laws, regulations, and standards that define the CMS working environment:

Security/Privacy Driver	Impact

Security/Privacy Driver	Impact
Legislative/Executive (Current)	
Health Insurance Portability and Privacy Act of 1996 (HIPAA)	Title I of HIPAA protects health insurance coverage for workers and their families when they change or lose their jobs. Title II of HIPAA, known as the Administrative Simplification (AS) provisions, requires the establishment of national standards for electronic health care transactions and national identifiers for providers, health insurance plans, and employers. It helps people keep their information private.
Federal Information Security Management Act (FISMA)	Requires each Federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.
Privacy Act of 1974	Establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of personally identifiable information about individuals that is maintained in systems of records by Federal agencies.
E-Gov Act of 2002	Its stated purpose is to improve the management and promotion of electronic government services and processes by establishing a Federal Chief Information Officer within the Office of Management and Budget, and by establishing a framework of measures that require using Internet-based information technology to improve citizen access to government information and services, and for other purposes.
State Laws	Specific IT security and privacy laws and regulations for the individual state of participating programs.
Health Information Technology for Economic and Clinical Health (HITECH) Act [part of the American Recovery and Reinvestment Act of 2009 (ARRA)]	Expands enforcement and the scope of businesses covered by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security regulations. The expanded privacy and security provisions contained within the Stimulus are expected to have a "significant impact" on a wide range of organizations that deal with, retain, use, and/or create protected health information.
Legislative/Executive (Pending)	
HHS Initial Guidance on the HITECH Act's Breach Notification Requirements (comments due May 21, 2009).	The HHS Guidance sets forth guidance concerning new rules applicable to HIPAA Covered Entities under Section 13402 of the HITECH Act (the “UPHI Breach Notice Rules”)
FTC Proposed Rule Requiring Consumer Notification of Security Breach for Electronic Health Information (comments due June 1, 2009).	The FTC Rule proposes new rules to apply to vendors of personal health records and other non-HIPAA covered entities dealing with “personal health records” (“PHRs”) within the meaning of the HITECH Act (the “PHR Breach Notice Rules”).
Health Information Technology Public Utility Act of 2009	Will facilitate nationwide adoption of electronic health records, particularly among small, rural providers. The

Security/Privacy Driver	Impact
	Health Information Technology Public Utility Act of 2009 will build upon the successful use of "open source" electronic health records by the Department of Veterans Affairs as well as the "open source exchange model," which was recently expanded among Federal agencies through the Nationwide Health Information Network-Connect initiative
Standards	
HIPAA Privacy Rules	The HIPAA Privacy Rule regulates the use and disclosure of certain information held by "covered entities" (generally, health care clearinghouses, employer sponsored health plans, health insurers, and medical service providers that engage in certain transactions.) It establishes regulations for the use and disclosure of Protected Health Information (PHI).
HIPAA Security Rules	The Security Rule complements the Privacy Rule. While the Privacy Rule pertains to all Protected Health Information (PHI) including paper and electronic, the Security Rule deals specifically with Electronic Protected Health Information (EPHI). It lays out three types of security safeguards required for compliance: administrative, physical, and technical.
Federal Information Processing Standards	Under the Information Technology Management Reform Act (Public Law 104-106), the Secretary of Commerce approves standards and guidelines that are developed by the National Institute of Standards and Technology (NIST) for Federal computer systems. These standards and guidelines are issued by NIST as Federal Information Processing Standards (FIPS) for use government-wide. NIST develops FIPS when there are compelling Federal government requirements such as for security and interoperability and there are no acceptable industry standards or solutions.
NIST Guidance	Special Publications in the 800 series present documents of general interest to the computer security community. The Special Publication 800 series was established in 1990 to provide a separate identity for information technology security publications. The Special Publication 800 series reports on NIST research, guidelines, and outreach efforts in computer security, and its collaborative activities with industry, government, and academic organizations. Many of the 800-series guidance are mandated under various FIPS, in particular FIPS 199, 200, and 201.
State Guidance	Specific IT security and privacy guidance for individual state of participating programs.
OMB Privacy & Security Guidance	OMB periodically issues security guidance for the handling of sensitive data and infrastructure and the reporting requirements of security programs. Examples are OMB memorandums A-123 and A-130.

Security/Privacy Driver	Impact
OMB FDCC Configuration Standards	The Federal Desktop Core Configuration (FDCC) is an OMB-mandated security configuration. The FDCC currently exists for Microsoft Windows Vista and XP operating system software.
CMS-Specific Data Sharing Requirements	Allows an employer, or insurer or agent on behalf of an employer, to electronically exchange health insurance benefit entitlement information.
CMS-Specific Privacy and Security Requirements (ARS and CMSRs)	A broad set of CMS security controls based upon NIST requirements. The ARS is periodically revised (usually annually) as a result of the mandate for the annually review of NIST Special Publication (SP) 800-53, *Recommended Security Controls for Federal Information Systems*.
Industry Standards and Workgroups	
NHIN Cooperative Technical and Security Core Services Work Group	Defines functional and technical specifications for key services to be used in implementing health information exchanges.
Draft Security Architecture Design Process for Health Information Exchanges (HIEs)	Provides a systematic approach to designing technical security architecture for the exchange of health information that leverages common government and commercial practices and applies them specifically to the HIE domain.
Federal Security Strategy for Health Information Exchange	Develops guidance that enables the adoption of secure, scalable health information exchanges among Federal and private sector healthcare organizations.
AHIC Confidentiality, Security and Privacy Work Group	Makes recommendations on the protection of personal health information in order to secure trust, and support appropriate interoperable electronic health information exchange.
Certification Commission for Health IT (CCHIT)	Private-sector collaboration launched by AHIMA, HIMSS, and the National Alliance to certify health IT products.
Health Information Technology Standards Panel (HITSP)	Public-private partnership chartered to identify, recommend, and harmonize data and technical standards for healthcare.
Health Information Security and Privacy Collaboration (HISPC)	Federal and state partnership working to harmonize laws and policies related to security and privacy.
Standards Development Organizations	Broad range of consortia, associations, and other bodies that create and maintain individual technical and data standards.
CONNECT	CONNECT is an open source software, built through collaboration of more than 20 Federal agencies, that connects organizations into the NHIN.

5. What challenges have you had to address in implementing these standards (e.g., training)?

Our most difficult issue is in determining the boundaries for implementation of various federal standards (such as FISMA.) The nature of CMS is to interface with private industry in order facilitate claims payments and to collect and distribute data. The basis of these connections is to provide for a better point-of-service experience for beneficiaries and to collect federally mandated transaction records and data sets. As systems and data are stretched out to these federal-commercial interfaces, the applicability of various federal standards becomes more difficult to determine. While federal standards typically provide for stronger security controls than industry standards, they also tend to drive up cost for our commercial partners. The definition of a "federal" system compared to the definition of a "commercial" system is increasingly dependent on contractual or business relationships rather than data content, particularly where data is aggregated commercially before it is transferred into Federal care (such as claims information.) These boundary issues are significant, as they determine the complexity of required controls, as well as the amount of direct (federal) oversight required for these systems.

While the extension of these boundaries can increase costs, the need for secure interfaces with our commercial partners (in addition to assurances of the security of their internal systems) is a must. Since the exploitation of CMS systems can be initiated through the compromise of commercial data or infrastructure, these security considerations are helping to drive our security posture now and into the future. As the complexity of exploits continue to grow, so must our diligence, and possibly the scope of CMS oversight and control.

6. ***What is the role/value of interoperable information security standards in helping to protect your business from data theft, loss, and misuse?***

The use of interoperable security standards are of tremendous advantage to CMS. However, CMS will always be held to the highest applicable standards. Today, that standard seems to be the FISMA requirements managed and maintained by NIST. So, while interoperable standards can be useful in ensuring minimum standards, they may not necessarily be sufficient for use throughout the CMS enterprise. In particular, CMS interfaces with industry may require certain trade-offs to ensure compatibility while still ensuring maximum compliance with Federal requirement. Therefore, simple adherence to commercial interoperability standards may not be sufficient for connectivity to the CMS infrastructure.

7. ***What are the current limitations or gaps in interoperable information security standards addressing data theft, loss, and misuse?***

Current limitations include minimum encryption standards. Under FISMA, encryption must meet minimum standards laid out by FIPS 140-2. Most commercial implementations of encryption do not meet this standard. Also, in many cases, the required "FIPS mode" for many application of encryption may impose undue interoperability restrictions with commercial or user clients. This standard can make it difficult to provide secure, yet compliant solutions.

Other gaps exist due to minimum e-authentication requirements for certain data types (under FISMA.) In particular, the required two-factor e-authentication for access to ePHI means that CMS must manage a significant amount of user accounts and provide sufficient

assurances that users are properly identified and authenticated before granting access to ePHI data.

8. What new and emerging issues around data theft, loss, and misuse do you foresee over the next 2-3 years?

In my opinion, the top emerging issue around data theft, loss, and misuse will involve providing access to sensitive information. CMS shares its sensitive information with over 7,000 various entities. These entities analyze CMS data to look for fraud, waste and abuse, perform healthcare research, process claims, and to find more efficient ways to provide service and care to our beneficiaries. The challenge from a security perspective is making sure these entities are performing their due diligence to protect the sensitive information. In our line of business, it is a constant challenge to find that balance between the enforcement of adequate security and processes and not inhibiting the business from functioning.